A System Safety Success: The Midcourse Space Experiment

by

Joyce A. McDevitt and Clayton A. Smith
Futron Corporation

INTRODUCTION

At 5:27 am Pacific Daylight Time on April 24, 1996, a McDonnell Douglas Delta II launch vehicle lifted off from Vandenberg Air Force Base (VAFB), California. On board was the Ballistic Missile Defense Organization's (BMDO) Midcourse Space Experiment (MSX). The MSX spacecraft was built by the Johns Hopkins University's Applied Physics Laboratory (JHU/APL) to study the phenomenology of target detection and tracking. This spacecraft program provided the authors with the opportunity to become involved with complex design, ground, and operational safety concerns in dealing with the use of liquid and solid hydrogen. The MSX program suffered a potentially dangerous failure in the plumbing associated with the hydrogen cryostat used in the spacecraft's main telescope, the Spatial Infrared Imaging Telescope (SPIRIT III). This paper discusses the failure and the adjustments made to the program. Had it not been for the thorough analysis and preventive systems put in place prior to performing ground operations, this leak could have resulted in a catastrophic loss.

MSX PROGRAM OVERVIEW

The MSX spacecraft is a BMDO project that offers major benefits for both the defense and civilian sectors. MSX represents the first system demonstration in space technology to identify and track ballistic missiles during their midcourse flight phase. The Sensor Technology Directorate of BMDO has overall responsibility for MSX.

The JHU/APL was contracted to develop, integrate, test, launch, and operate the MSX spacecraft and several of its primary sensors. Futron Corporation was subcontracted to perform the system safety function for JHU/APL. MSX was launched aboard a McDonnell Douglas Delta II booster from VAFB. The launch vehicle placed the spacecraft in an approximately 900 kilometer, high inclination, circular, near-Sun synchronous orbit.

MSX experiments provide critical first-time observations of missile target signatures against earthlimb, auroral, and celestial-cluttered backgrounds. MSX can be pointed so that all its instruments simultaneously view the Earth's atmosphere in any direction, and it offers scientists an opportunity to study the composition, dynamics, and energetics of the atmosphere, including small annual changes in such chemicals as ozone, carbon dioxide, and chlorofluorocarbons. Global atmospheric changes following major solar disturbances and environmental events such as volcanic eruptions, forest fires, and agricultural burnoffs can also be monitored.

MSX SPACECRAFT

The MSX spacecraft was built and integrated at the JHU/APL facility in Laurel, Maryland. The MSX spacecraft (Figure 1) has a 1½ meter square cross section, is 5 meters long, and weighs 2,700 kilograms. Two solar arrays provide 1,200 Watts of power and a 50 amp-hour nickel-hydrogen (NiH_2) battery provides 28 volts direct current. The operational lifetime of the spacecraft is expected to be four years with cryogen life of 18 months.

The spacecraft consists of three main sections: the instrument section, the truss section, and the electronics section. The instrument section houses 11 optical sensors, precisely aligned so that target activity can be viewed simultaneously by multiple sensors. The electronics section contains the majority of the spacecraft bus and

the warm electronic portions of the instruments. These two sections are separated by the mid-section, a graphite epoxy truss.

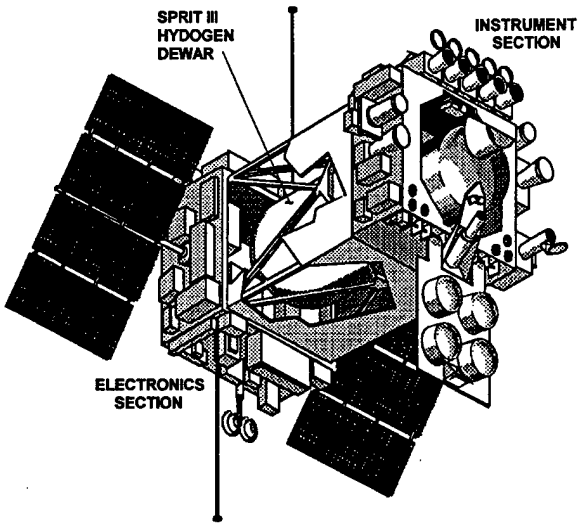

Figure 1. MSX Spacecraft

The mid-section supports the spacecraft's primary instrument, SPIRIT III (developed by the Space Dynamics Laboratory of Utah State University). SPIRIT III is a large advanced cryogenically-cooled long-wave infrared sensor. The cooling system incorporates a vacuum-enclosed container, or dewar, of cryogenic coolant to chill the sensor to operating temperatures far below zero degrees Fahrenheit. The dewar, containing 944 liters of frozen hydrogen at approximately 9°K (-443°F), keeps the telescope's optics and internal electronics between 13°K and 20°K. The thermal design of the mid-section maintains the outer shell of the dewar at approximately 200°K. The 200 centimeter long truss thermally isolates the heat-sensitive instrument section from the much warmer spacecraft bus.

The other instruments on board the spacecraft include: UVISI (Ultraviolet and Visible Imagers and Spectrographic Imagers), SBV (Space-Based Visible) instrument, and many contamination experiments that examine the environment near the spacecraft.

Pre-launch and launch operations were performed at VAFB. These included spacecraft transportation, processing, testing, vehicle and payload mating, pre-launch checkout and launch. The MSX Program used the Astrotech Space Operations' Payload Processing Facility (PPF), Spacecraft Payload Control Center (PCC), and NASA's Space Launch Complex-2 West (SLC-2W).

SYSTEM SAFETY PROGRAM

The system safety program for MSX established the safety function within the overall program, detailed the responsibilities, and outlined safety requirements to assure safety for the entire life cycle of the spacecraft, from design through the end of the mission. Safety management and engineering were integrated with the overall MSX Program activities involving system design, integration, test, transportation, pre-launch, launch and space test operations in order to minimize accident risks to personnel, the MSX spacecraft, the launch vehicle, ground support equipment (GSE), facilities and property, other spacecraft, and the environment.

As spacecraft integrator, JHU/APL was the focal point for all system safety activities on the program. The safety program comprised elements of JHU/APL, Utah State University's Space Dynamics Laboratory (USU/SDL), Lockheed Missiles and Space Company (LMSC), Massachusetts Institute of Technology's Lincoln Laboratory (MIT/LL), 30th Space Wing (30 SW), Astrotech Space Operations (ASO), NASA Kennedy Space Center (KSC), NASA Goddard Space Flight Center (GSFC), Consolidated Space Test Center, and McDonnell Douglas Aerospace.

Under contract to JHU/APL, Futron Corporation managed the safety program, developed all of the safety documentation and provided on-site safety support at GSFC and VAFB. While the spacecraft was at the range, Futron Corporation provided on-site safety oversight for all hazardous procedures and was the main interface between the federal range safety and facility safety organizations and the program. The safety documentation process involved developing a number of deliverables for the 30 SW and NASA including:

- *MSX Integrated Safety Program Plan* established the safety organizational relationships, responsibilities, and safety management and engineering activities that assured a comprehensive accident risk assessment program.

- *MSX Preliminary Hazard Analysis* provided an initial assessment of safety risks associated with the MSX spacecraft design and ground and flight operations.

- *MSX Ground Safety Plan for Spacecraft Operations at GSFC* established the operational safety requirements for thermal vacuum and environmental testing operations at the Goddard Space Flight Center.

- *MSX Ground Safety Plan for Spacecraft Operations at VAFB* established the operational safety requirements for pre-launch operations at the Astrotech Payload Processing Facility and integration of the spacecraft with McDonnell Douglas Aerospace's Delta II launch vehicle at SLC-2W.

- *MSX Accident Risk Assessment Report for Spacecraft Operations at VAFB* provided evidence of safety requirements compliance and the acceptability of safety risks in order to receive the range safety approvals for ground processing and launch.

- *MSX Test Operations Risk Assessment* documented the mishap risks associated with the operation of the MSX spacecraft in orbit.

- *Hazardous Procedures* documented the operational steps and safety requirements to be followed, safety equipment needed for the operation, and emergency contingencies for all hazardous activities involving the processing of the spacecraft.

SYSTEM SAFETY APPROACH

The principal document for reporting safety results between the program and the 30 SW was the Accident Risk Assessment Report (ARAR). It documented the hazards and residual risks associated with the spacecraft and the operations involved in processing the spacecraft at VAFB before launch and including the launch phase up to orbital insertion. The process began by submitting a Preliminary Hazards Analysis (PHA) as an introduction to the hazards, with explanations of energy sources and descriptions of generic hazards. Later the ARAR was completed with the insertion of hazard controls and associated verifications.

The approach taken to perform the hazards analyses for the MSX program consisted of the following phases:

1. Validation of compliance with all applicable requirements specified in WSMCR 127-1 using checklists,
2. Development of detailed system descriptions,
3. Performance of a PHA, including development of a Preliminary Hazard List (PHL) to analyze each system/instrument for known hazard categories,
4. Development of system level hazards analysis as appropriate to analyze for hazards associated with flight hardware, ground support equipment, personnel and facility interfaces,
5. Development of hazard reports in updating the PHA to determine the causes, controls, and methods of verification that the control was in fact implemented, and
6. Development of fault trees to analyze specific hazards with catastrophic potential effects.

The hazard reports were used to define and qualify the risks to the program. The risk was defined in terms of severity and probability. These figures of merit were taken from those used in Mil-Std-882B. The initial risk for each of the 100 hazards (prior to control implementation) was provided as was the residual or final risk (after control implementation). In order to illustrate the results of the controls implemented to minimize the hazards, the risk profiles in Table 1 are presented so the initial risk may be compared to the residual risk. While the severity of most hazards remained the same, the probability of occurrence decreased dramatically.

Table 1. Risk Profiles

Initial Overall Program Risk

	A	B	C	D	Total
I	2	17	18	6	43
II	3	7	7	--	17
III	5	7	15	3	30
IV	--	2	7	1	10
Total	10	33	47	10	100

Residual Overall Program Risk

	A	B	C	D	Total
I	--	--	11	32	43
II	--	--	4	10	14
III	--	2	12	18	32
IV	--	--	2	9	11
Total	--	2	29	69	100

Severity levels are: I) catastrophic, II) critical, III) marginal, and IV) negligible.
Probability levels are: A) frequent, B) occasional, C) rare, and D) improbable.

The System Level Hazard Matrix (Table 2) illustrates the distribution of the hazards with respect to the systems and the hazard categories. The GSE was separated into those hazards associated with the typical spacecraft GSE and those related to cryogenic GSE.

Most of the hazards identified were typical for spacecraft. These included electrical hazards dealing with high voltage power supplies, batteries, deployable mechanisms, ordnance, lifting operations, and operations of RF transmitters. The main concern for this spacecraft was that of fire and explosion mainly due to operations with the hydrogen. The spacecraft was relatively benign with the exception of the hydrogen and the activities associated with the filling of the dewar, solidification of the hydrogen and subsequent spacecraft operations. From the perspective of the contributing systems, the combination of the SPIRIT III instrument including its dewar and GSE, made up 32% of the hazards identified.

SPIRIT III FAILURE

On November 2, 1994, the SPIRIT III instrument suffered an internal rupture. The failure resulted in melting, vaporizing, and venting of approximately 160 pounds of solid hydrogen outside the PPF and the evacuation of the facility. Although the instrument was damaged, no personnel were injured, the PPF was not damaged, and no other part of the spacecraft was damaged.

This section describes briefly the design of the SPIRIT III instrument, its safety systems, the failure causes, and the modifications made after the failure.

SPIRIT III Cryostat Description

This system description is presented to give a basic understanding of the equipment, operating procedures and environmental parameters involved. It is not intended to be a complete tutorial on the design and operations of SPIRIT III.

Table 2. System Level Hazard Matrix

	Acceleration	Asphyxiation	Corrosion	Electrical	Fire / Explostion	Impact	Ionizing Radiation	Non-Ionizing Radiation	Pressure	Temperature	Toxic	
Structure	2											2
Power			1	6	1	1			1			10
Thermal Control				1					1			2
RF Communication						3		2				5
Attitude Control	1			1				1				3
SPIRIT III				1	6	1		1	3		1	13
UVISI						1						1
Reference Objects						1						1
SBV						1						1
Contamination Experiment				2		1	1	2	1		1	8
Ordance					2							2
System Interfaces	2	1		3	2	4						12
Spacecraft GSE	2	1		3	5	4	1	3	1	1		21
Cryogenic GSE	1	1		1	13				2	1		19
	8	3	1	18	29	17	2	9	9	2	2	100

SPIRIT III has two major parts: a telescope system and a cryogen system. The telescope and internal electronics (radiometer and interferometer) operate in a temperature range of 13°K to 20°K. In order to maintain temperatures that low, the telescope is thermally linked to a cryogen system (also referred to as the cryostat) containing a dewar. The dewar contained approximately 160 pounds of solid hydrogen.

Figures 2 and 3 show the exterior of the SPIRIT III assembly and a schematic of this configuration. The main part of the cryogen system is the dewar. The dewar is a 40½-inch diameter cylindrical tank with domed ends. The tank is partially filled with an open-cell 1.5 to 3.0 percent dense aluminum foam. The foam prevents movement of the solid hydrogen within the tank during spacecraft slew operations and acted to greatly reduce temperature differentials in the tank as the hydrogen sublimes away from the tank wall. To reduce parasitic heat loads into the tank, the cryostat features two vapor-cooled shields, and on orbit, a passively cooled (200°K) external vacuum shell. Throughout ground processing, the vacuum shell remains at ambient temperature. The cryostat provides temperature sensors to monitor the status of the cryogen.

Figure 4 shows the plumbing schematic for the SPIRIT III cryostat. This was the configuration of the cryostat prior to the failure. There are five penetrations into the dewar; hydrogen fill and vent lines, helium cooling inlet and exit lines, and an orbit vent (only used on orbit). The hydrogen and helium lines are protected with a burst disk/check valve assembly and shared a common outlet, the emergency vent line. The orbit vent was capped (later changed) during ground processing with two pyro vent valves to be opened on orbit. The vacuum space between the dewar and outer shell is also protected with a burst disk/check valve in case the tank ruptured inside the outer vacuum shell. Inside the tank are the liquid helium cooling coils used to solidify the liquid hydrogen.

The procedure used to cool SPIRIT III to operating temperature required the dewar to be pre-cooled and then filled with 160 pounds of hydrogen. The dewar was pre-cooled by filling it with liquid helium. Once the temperature stabilized, the helium was purged and the dewar was filled with liquid hydrogen.

Filling the cryostat was a two step process. First, approximately 130 pounds of liquid hydrogen were transferred into the dewar. This liquid was then frozen by flowing liquid helium through coils internal to the cryostat. During the solidification process, the hydrogen condensed. The ullage was then filled with 30 pounds of hydrogen using

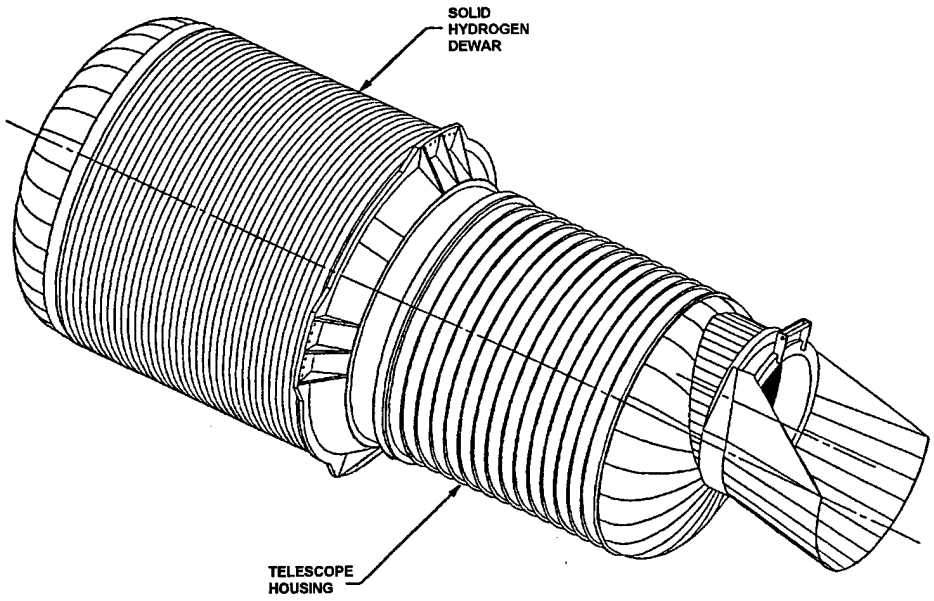

Figure 2. SPIRIT III Exterior

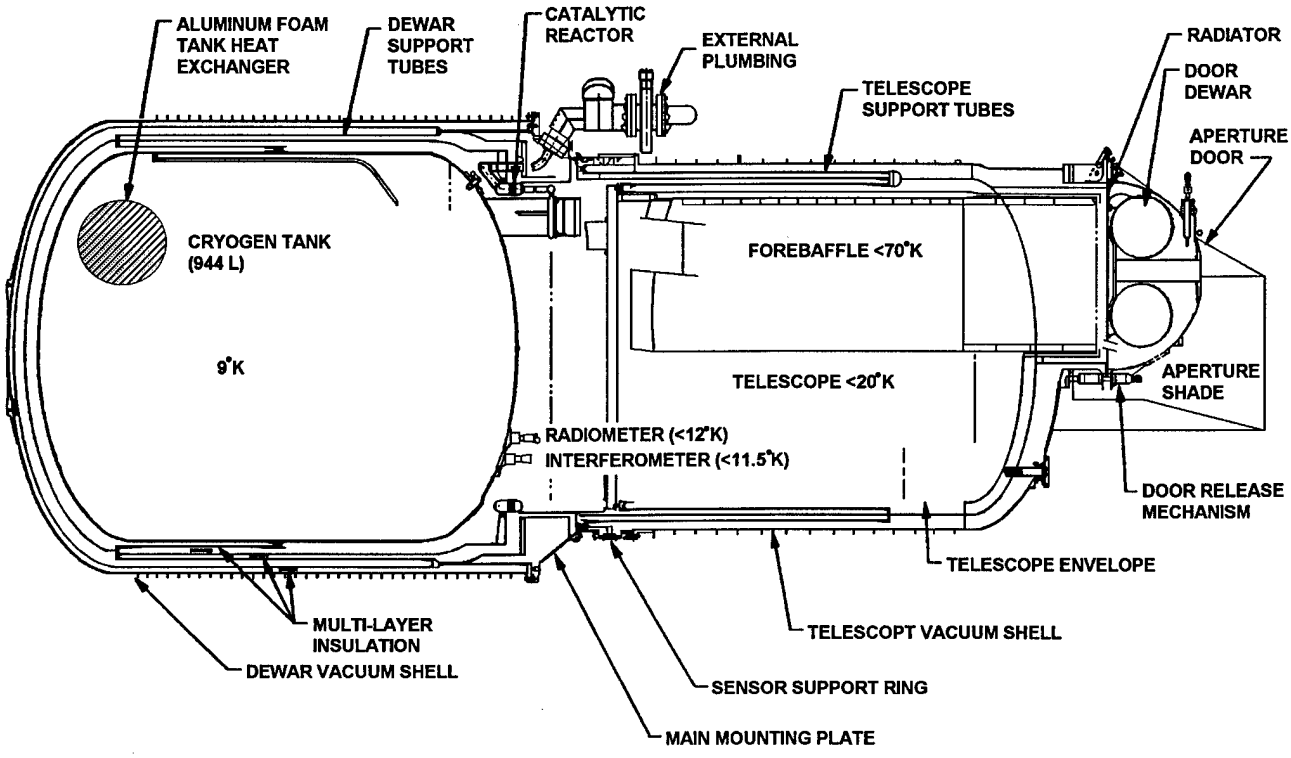

Figure 3. SPIRIT III Internal Schematic

a gas phase top-off procedure (step two). Approximately 2 pounds of hydrogen were transferred each day for 15 days by adding cold gaseous hydrogen. The gaseous hydrogen solidified in layers on the already frozen hydrogen in the tank to fill the ullage space.

This top-off procedure was intended to add several months of lifetime to the instrument. However, there were penalties associated with this procedure. First, with the ullage space filled completely, there was no room for the hydrogen to expand if it warmed. Second, the gas phase top-off increased the operational risk because the hydrogen tank connections were opened and closed an additional 11 times.

Failure Scenario

A formal failure analysis was conducted. During equipment breakdown and repair, a picture of the failure scenario emerged. A solid hydrogen plug had formed in the orbit vent line trapping hydrogen gas between the plug and the capped end. Concurrently (and independently), a small leak had developed in this line between the plug and the tank. The leak caused the pressure and temperature to rise in the vacuum space and also in the trapped portion of the orbit vent line. Eventually the pressure rise in that portion of the line ruptured its weakest link, the catalytic converter.

A brief description of the events on the day of the failure is given followed by a discussion of the failure causes.

The hydrogen tank had been filled and "topped-off", the liquid helium used to maintain the solid hydrogen had been disconnected, and the spacecraft was undergoing final system checks and close-out procedures. The program was within three days of moving to the launch pad for integration with the launch vehicle and three weeks of launching.

During trouble-shooting to try to understand an anomalous reading in the tank pressures, creaking and ruffling sounds originating from the cryostat were heard. Less than two minutes after that, there was a loud "pop" sound emanating from the cryostat. The monitoring system indicated that the dewar and telescope temperatures were rising rapidly. This was the primary indication that a major malfunction had occurred. The lead cryogen engineer immediately recognized the gravity of this indication and ordered

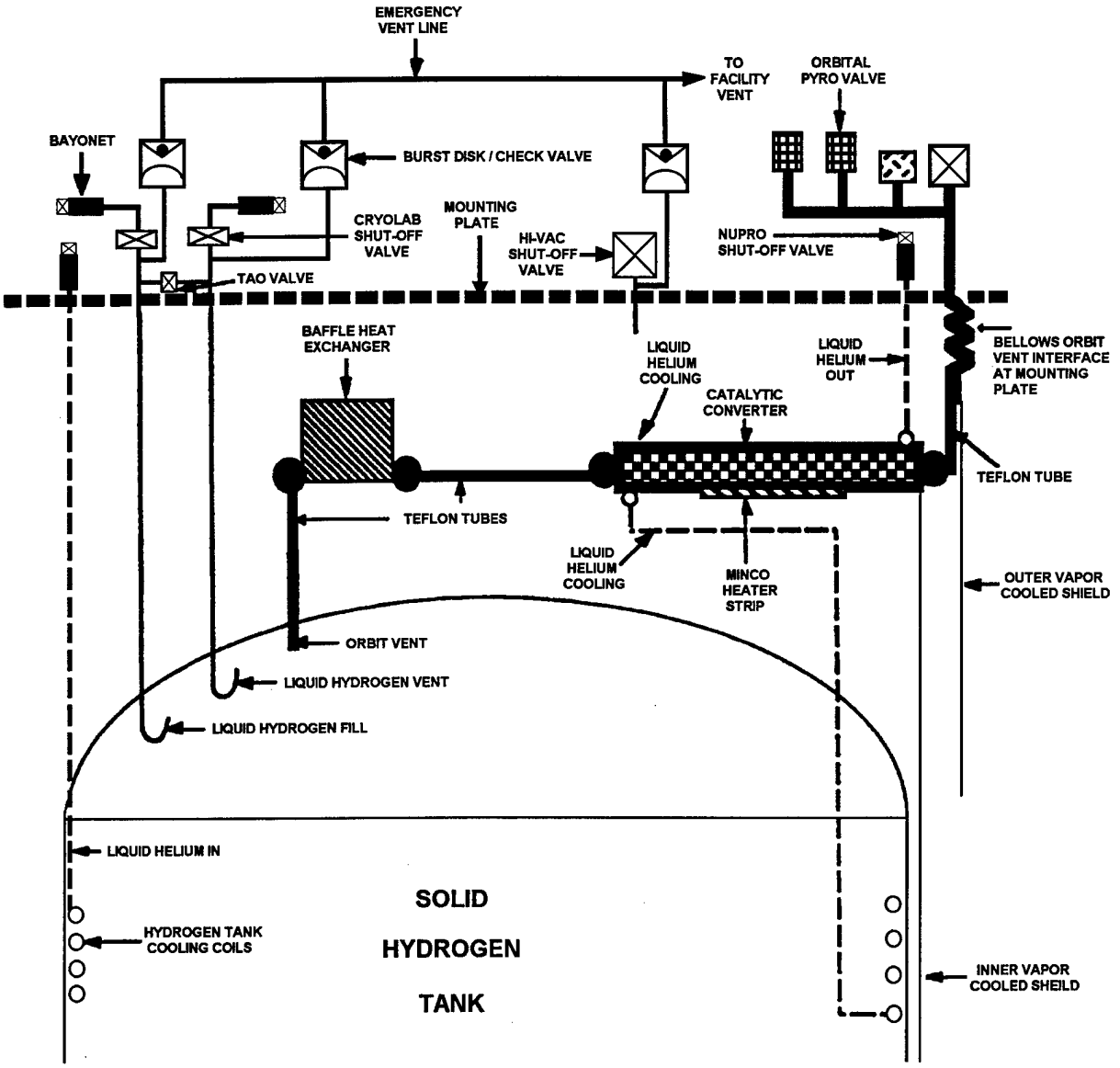

Figure 4. Cyrostat Plumbing Schematic

everyone to evacuate. The PPF was cleared and all power was shut down. This "pop" was discovered later to be the rupture of the plumbing and catalytic converter.

After several minutes the cryogen engineers reentered the PPF to check the status of the spacecraft when the facility hydrogen detectors indicated no evidence of a hydrogen leak. The local hydrogen sensors gave no indication of hydrogen venting from the cryostat, and there was no indication of frost forming on the vacuum shell. With the GSE power shut off, only the temperature could be monitored. The temperature monitoring equipment indicated that the internal tank skin temperature was 18°K, well above the 13.8°K triple point temperature (the point where the temperature remains constant while the heat input is used to melt a solid mass). This implied that the tank was subjected to significant heat loads, sufficient to sustain film boiling between the tank wall and the triple point cryogen, or events had occurred to create a new equilibrium situation for the tank (i.e., the cryogen had melted at the triple point and at least locally had warmed to the 18°K skin temperature). At that time there was no evidence suggesting that the hydrogen had vented through the emergency vent system.

An irreversible process had started. The hydrogen was melting, and the pressure inside the cryostat was rising and would eventually rupture a burst disk and begin venting. There was nothing the engineers could do until the hydrogen had completely melted and vented through the emergency vent. The base fire department arrived and the PPF was closed off.

The following morning the team noticed that the exterior vent stack was covered with ice from the base to a height of approximately 20 feet high indicating that cold hydrogen gas had been and could still be venting from the cryostat. Prior to entering the PPF, the facility hydrogen sensors were used to verify the safety of re-entering the building and the cryogen and safety engineers returned to the servicing bay to assess the damage. A local hydrogen sensor indicated there was some hydrogen gas leaking from a burst disk check valve assembly, but the facility ceiling sensors were not detecting any, indicating that the leak rate was very small. This leak disappeared as the assembly warmed and an o-ring joint between the spacecraft and burst disk thawed.

The frosted condition of the emergency vent line and vacuum shell suggested that the tank had not completely vented, but the data acquisition system temperature readouts indicated the flowrates had dropped to insignificant levels.

Hydrogen sensors in the vacuum module, GSE used to pumpdown the vacuum space, confirmed that the inner tank was communicating with the vacuum space. The cryogen team then started to purge the tank with nitrogen to drive off any remaining hydrogen. The pressure was monitored throughout the pumpdown, with special care taken to assess whether there was any slowdown, indicating the presence of water vapor. There was absolutely no slowdown observed confirming that the outer vacuum shell was not leaking to ambient atmosphere as a consequence of this anomaly.

The most plausible theory suggests there were two anomalies required to cause the failure; lines plugged with solid hydrogen and a leak. The first anomaly was the formation of solid hydrogen plugs in one of the two thermally isolated Teflon tubes in the orbit vent line. The formation of these hydrogen plugs in the orbit vent line was not recognized as a potential problem for a number of reasons:

- No flow rate in this section of plumbing. Therefore, any gas in this section of plumbing would be at the vapor pressure associated with the liquid fill, the gas top-off and the partial pressures of the solid hydrogen during the recool operations.
- Low thermal capacity in the plumbing compared to the main tank. Any gas that was in the plumbing would be naturally cryopumped back into the main tank rather than remain in the plumbing.
- Low thermal inputs to the system. Any hydrogen-related partial blockages or plugs would slowly warm and cryopump back to the main tank. Overpressure of the system in this condition was not considered an issue.
- Any partial or total blockage would be easily cleared on orbit, a low lifetime penalty.

The second anomaly was a leak in a Teflon tube that allowed a higher heat load to the internal cryostat plumbing. With the high heat loads, the warming solid hydrogen trapped within the orbit vent lines sublimed, building pressure until the components failed.

What may never be known is where and why the leak occurred. Several possibilities exist. The leak could have been related to the solidification of hydrogen within the orbit vent plumbing or related to thermal fatigue associated with the constant reloading of the dewar with liquid helium. The other possibilities suggest that the leak was a result of a thermal blanket bracket impinging on the internal flight cryostat plumbing. If a bracket impinged on a Teflon tube, the Teflon could eventually "cold flow" and weaken. Analysis of the hydrogen line on the baffle thermal link also showed evidence of stress corrosion.

It should be noted that, while the exact cause of the potential failure event was not discovered by hazard analysis prior to the incident, the results of this failure scenario were addressed in the fault tree analysis. The safety systems were designed and implemented to minimize the risk, firstly to personnel, and secondly, to the facility and spacecraft associated with loss of cryostat integrity.

Safety System Description

The safety systems associated with the spacecraft and its GSE include the hydrogen detection system, cryostat data monitoring system, the emergency vent system and the power termina-

tion system. All these systems operated as designed during normal operations and during the failure event. Without these system the consequences of the failure would have been catastrophic.

Hydrogen Detection System

For ground operations in the PPF, four sets of hydrogen sensors monitored the Lower Explosive Level (LEL) to provide detection and early warning of hydrogen leaks. None of the sensors detected hydrogen prior to or at the time of the failure. In addition, the hydrogen sensors confirmed the existence of a safe environment prior to personnel reentering the highbay after the failure. There were:

Module Sensors - Two module sensors were located inside the cryogen GSE (one each in the vacuum and gas modules). They were designed to sense hydrogen in the cabinet external to its plumbing.

Hand Held Sensor - A hand held sensor was used during all operations where hydrogen was flowing and for emergency use during all other cryogen operations.

Local Level Sensors - The local level sensor system (nine sensors) monitored the local area around the plumbing joints to support hydrogen operations. It indicated small leaks so that actions could be taken before a larger problem developed. To increase their sensitivity, the sensors were placed in hoods that collected and concentrated the hydrogen gas. This system provided remote monitoring from the Payload Control Center for safe reentry following an evacuation.

Facility Sensors - Four facility sensors were connected to the facility HVAC and power system. At sensing 10% LEL, an audible alarm would sound in the control room and the pneumatically operated roof damper would open and allow the outside air to be brought in through the HVAC system to dilute the concentration of hydrogen in the highbay. At 25% LEL, an alarm would sound, power would terminate at the non-explosion proof receptacles, the fire department would automatically be called, and the HVAC system would fully open the roof louvers.

Cryostat Data Monitoring System

The Cryostat monitoring system consisted of the Data Acquisition System (DAS) and the Temperature, Monitor, and Alarm (TM&A) unit. The DAS recorded various temperatures throughout the SPIRIT III Telescope and Cryostat. In addition, SPIRIT III personnel recorded data every half hour from the gages and indicators on the GSE modules, monitored the equipment continuously and responded to all anomalies. The explosion-proofed, battery-operated TM&A monitored hydrogen tank temperatures with an alarm point set to alert personnel. This equipment and the personnel monitoring the operations provided advance notice of possible venting so that action could be taken, either preventing the system from venting or securing the facility for venting. This system performed as designed during the failure providing an early warning to evacuate the PPF.

Emergency Vent System

The emergency vent system was designed so that during an emergency the hydrogen in the cryostat would be safely vented outside the facility.

The vent system (see Figure 5) consists of a plumbing cluster external to the hydrogen tank, a 2-inch diameter vacuum-jacketed flexhose, and a vent stack outside the facility. The flexhose connects the plumbing cluster on the spacecraft to the vent stack by penetrating the wall of the building. The stack includes a 35-gallon liquid reservoir (to catch any liquid hydrogen) with a stack extending above the roof to safely vent the hydrogen. A catch basin was located at the base of the stack to contain any liquid air runoff on the outside. The stack is terminated with an atmospheric isolator and low ESD emission vent tip. A constant gaseous helium purge is supplied to inert the stack.

The only anomaly noted with the vent system was a small hydrogen leak at the main tank burst disk. Because the vacuum jacketing at this joint was less than other places, an o-ring in the joint froze allowing some hydrogen gas to leak into the facility. This leak, as measured with the portable hydrogen monitor, was not significant. The monitor indicated a hydrogen gas presence but would not provide a steady state reading or identify the exact leak location. Several other flex-

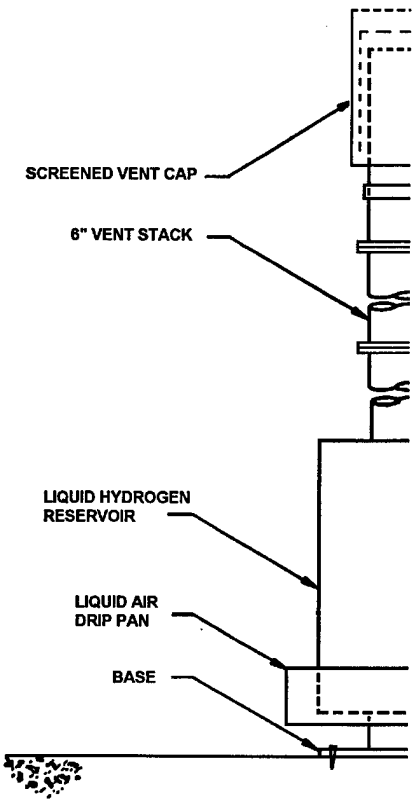

Figure 5. Emergency Vent Configuration

hose joints showed signs of icing, but no leaks could be detected.

Power Termination System

The facility electrical system was designed to automatically terminate power to the non-explosion proof receptacles when the roof mounted facility hydrogen sensors reached 25% of the LEL for hydrogen. Additionally, power distribution units in the highbay and control room provided a single point shut off in each area to terminate electrical power to spacecraft GSE in the event of an emergency. The necessity to shutoff these power distribution units was stressed in the operational briefings given to all personnel.

Aftermath

Three main actions resulted from this failure;

1) SPIRIT III was removed from the spacecraft, taken apart, and reworked,
2) Hydrogen filling procedures were revised, and
3) All the safety analyses and safety systems were reviewed.

It is beyond the scope of this paper to detail all of the changes to the hardware and procedures. A failure investigation team from BMDO and a separate investigation team from USU/SDL and LMSC researched the design, materials, physics, failure modes, quality systems, and manufacturing techniques. The output of that process was a new configuration of the internal plumbing, specifically the addition of a burst disk check valve assembly on the orbit vent line. Another major consequence was that the "Gas Phase Top-Off" procedure was deleted to assure adequate ullage for hydrogen expansion.

All of the hazard reports concerning the cryostat and its associated GSE were reexamined in light of the failure and the redesign effort. The hazard reports were updated with new design and verification documentation. It was determined that the safety systems performed as designed and therefore no modifications were made to them. However, changes were implemented regarding the daily activities of the safety engineers, namely, an increased presence during non-hazardous operations and increased vigilance on the daily inspection of the safety systems.

The one safety system that needed attention related to PPF emergency egress and involved the air shower door, and personnel response. When the order was given to evacuate the high-bay, the personnel in the room proceeded to the air shower door (the door used to enter the high-bay) instead of the three emergency exits. Once the first person went through the door, the air shower turned on and locked the door to the highbay for about 15 seconds (normal operation for the air shower). This interlock prevented any other people from using this exit until the interlock disengaged. The interlocking door feature of the air shower was disabled, a larger sign was posted noting that it was not an emergency exit, and this point was strongly emphasized during the safety retraining given to all personnel.

MISSION RESULTS

After more then a year of investigation, redesign, and rework, the MSX program resumed field activities on January 1, 1996. SPIRIT III was placed back into the spacecraft and filled with

hydrogen. MSX successfully launched on April 24, 1996.

MSX has performed well. A press release dated 5 March 1997 states that the MSX has tracked two medium-range missiles, known as Low Cost Launch Vehicles. The flights were launched from the NASA Wallops Flight Facility, Wallops Island, Va., each on a 135-degree azimuth. The first launch occurred February 12, 1997 and the second launch occurred on February 23, 1997. These flights demonstrated the ability of space-based optical sensors on MSX to perform key missile defense functions - acquisition, tracking and discrimination in the mid-course phase of missile flight - on realistic targets against realistic backgrounds.

CONCLUSION

Implementing a successful safety program for the MSX, a complex hazardous system, required good planning, thorough analysis and follow-up, operational discipline, and management support. This was accomplished and enhanced by the outstanding technical capability and teamwork across the entire program including the customer, subcontractor, range, PPF, and launch vehicle personnel. The design and safety engineers from all these organizations worked together to solve difficult problems to ensure a successful and safe campaign.

The design of the safety systems was derived from a thorough understanding of the consequences of a failure and a comprehensive examination of the various mitigation measures for preventing and containing them. The hazard analyses performed to reach this understanding was the result of excellent communication among all the parties of the program team. The program also benefited from having the same safety team in place for over six years from conceptual design through launch. This allowed the safety engineers on-site at the range to be fully aware of all the possible hazards and consequences from both an engineering and operational viewpoint.